# Group Assignment
# Comp Sci 361: Information Assurance and Security
# Full marks: 35
# Submission Deadline: 11/28/2021

In this assignment you will work in groups of 3/4 students. Most of the deliverables are drawn from the section 1 and 2 of the following labs

Lab 8: Performing a web site and database attack by exploiting identified vulnerabilities

Lab 9: Eliminating threats with a layered security approach

Lab 10: Implementing an information systems security policy

While you have already completed section 1 of lab 9, you are required to complete section 2 of lab 8 and both section 1 and 2 of labs 9 and 10.

The tasks in sech section that you need to complete are listed below

## Lab 8 Section 2

*Screen captures of the followings*

a) XSS form showing `yourname`;
b) XSS form showing the vulnerability pop-up alert;
c) submissions that return a response for scripts used to determine the number of columns in a table;
d) submissions that return a response for scripts seeking the correct spelling of a field name;
e) submissions that return a response for scripts that search for a possible hit on the database's characters;
f) SQL injection user hash information;

*Additional Component*

a) Create a SQL injection attack to determine the correct field name that holds the user's surname

*Bonus mark*

As you discovered in this lab that the password hash was included in the `mysql.user` database; however, there is another database that contains user data. What is the name of that database, and what content can you uncover within it

# Lab 9 Section 1

*Screen captures of the followings*

a) Virus details;
b) Emptied Quarantine area (Virus Vault);
c) Updated services list;
d) Updated File and Printer Sharing rule in the firewall;
e) Inbound FileZilla Server rule;

# Lab 9 Section 2

*Screen captures of the followings*

a) AVG Detection window;
b) Additional threat details;
c) Emptied Quarantine area (Virus Vault);
d) Updated services list;
e) Updated Email and accounts rules in the firewall;
f) Outbound FileZilla Server rule;

*Additional Component*

Research Windows services. Using the screen captures you made in Part 2 (disabling unwanted services) of the lab, identify at least three additional services that could be disabled safely. Explain your choices.

# Lab 10 Section 1

*Screen captures of the following*

a) newly configured Domain Password Policy;
b) newly configured Account Lockout Policy;
c) student user account logged on to `TargetWindowsMem03`;
d) Administrator account logged on to `TargetLinux`;

*Additional Component*

a) In this lab, you changed the Audit Policy to record both successful and unsuccessful login attempts. What drawbacks do you foresee when Auditing is enabled for both success and failure?

# Deliverables

1) **Report** with all the screen shots required for each task. The report should also include the procedure(s) you followed to solve the additional components and the results you obtained (if any). Use screen shots to present your results from the additional components.
2) **Peer review report** should include your reflection of the group assignments including any challenges you faced while addressing the additional components and your mitigation policies to address the challenges. You are required to comment on your group member's work, participation, and cooperation.
3) **Bonus** component can be completed by the groups. However, it is optional. There won't be any penalty for not doing it. You can earn a reward up to 5% bonus mark towards your final grade. Group members will be assessed based on the report and the peer review report.